Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'cryptsetup-luksDump.8' command

$ man cryptsetup-luksDump.8

CRYPTSETUP-LUKSDUMP(8)   Maintenance Commands   CRYPTSETUP-LUKSDUMP(8)

NAME

cryptsetup-luksDump - dump the header information of a LUKS device

SYNOPSIS

cryptsetup luksDump [<options>] <device>

DESCRIPTION

Dump the header information of a LUKS device.

If the --dump-volume-key option is used, the LUKS device volume key is dumped instead of the keyslot info. Together with the --volume-key-file option, volume key is dumped to a file instead of standard output.

Beware that the volume key cannot be changed without reencryption and can be used to decrypt the data stored in the LUKS container without a passphrase and even without the LUKS header. This means that if the volume key is compromised, the whole device has to be erased or reencrypted to prevent further access. Use this option carefully.

To dump the volume key, a passphrase has to be supplied, either interactively or via --key-file.

To dump unbound key (LUKS2 format only), --unbound parameter, specific --key-slot id and proper passphrase has to be supplied, either interactively or via --key-file. Optional --volume-key-file parameter enables unbound keyslot dump to a file.

To dump LUKS2 JSON metadata (without basic header information like UUID) use --dump-json-metadata option.

<options> can be [--dump-volume-key, --dump-json-metadata, --key-file,

--keyfile-offset, --keyfile-size, --header, --disable-locks,

--volume-key-file, --type, --unbound, --key-slot, --timeout].

WARNING: If --dump-volume-key is used with --key-file and the argument

to --key-file is '-', no validation question will be asked and no

warning given.

OPTIONS

--type <device-type>

Specifies required device type, for more info read BASIC ACTIONS

section in cryptsetup(8).

--key-file, -d name

Read the passphrase from file.

If the name given is "-", then the passphrase will be read from

stdin. In this case, reading will not stop at newline characters.

See section NOTES ON PASSPHRASE PROCESSING in cryptsetup(8) for

more information.

--keyfile-offset value

Skip value bytes at the beginning of the key file.

--keyfile-size, -l value

Read a maximum of value bytes from the key file. The default is to

read the whole file up to the compiled-in maximum that can be

queried with --help. Supplying more data than the compiled-in

maximum aborts the operation.

This option is useful to cut trailing newlines, for example. If

--keyfile-offset is also given, the size count starts after the

offset.

--volume-key-file, --master-key-file (OBSOLETE alias)

Use a volume key stored in a file. The volume key is stored in a

file instead of being printed out to standard output.

--dump-json-metadata

For luksDump (LUKS2 only) this option prints content of LUKS2

header JSON metadata area.

--dump-volume-key, --dump-master-key (OBSOLETE alias)

Print the volume key in the displayed information. Use with care,
as the volume key can be used to bypass the passphrases, see also
option --volume-key-file.

--key-slot, -S <0-N>

For LUKS operations that add key material, this option allows you
to specify which key slot is selected for the new key.

The maximum number of key slots depends on the LUKS version. LUKS1
can have up to 8 key slots. LUKS2 can have up to 32 key slots based
on key slot area size and key size, but a valid key slot ID can
always be between 0 and 31 for LUKS2.

--timeout, -t <number of seconds>

The number of seconds to wait before timeout on passphrase input
via terminal. It is relevant every time a passphrase is asked. It
has no effect if used in conjunction with --key-file.

This option is useful when the system should not stall if the user
does not input a passphrase, e.g. during boot. The default is a
value of 0 seconds, which means to wait forever.

--header <device or file storing the LUKS header>

Use a detached (separated) metadata device or file where the LUKS
header is stored. This option allows one to store ciphertext and
LUKS header on different devices.

For commands that change the LUKS header (e.g. luksAddKey), specify
the device or file with the LUKS header directly as the LUKS
device.

--disable-locks

Disable lock protection for metadata on disk. This option is valid
only for LUKS2 and ignored for other formats.

WARNING: Do not use this option unless you run cryptsetup in a
restricted environment where locking is impossible to perform
(where /run directory cannot be used).

--unbound

Dumps existing LUKS2 unbound keyslot.

--batch-mode, -q

Suppresses all confirmation questions. Use with care!

If the --verify-passphrase option is not specified, this option also switches off the passphrase verification.

--debug or --debug-json

Run in debug mode with full diagnostic logs. Debug output lines are always prefixed by #.

If --debug-json is used, additional LUKS2 JSON data structures are printed.

--version, -V

Show the program version.

--usage

Show short option help.

--help, -?

Show help text and default parameters. == REPORTING BUGS

Report bugs at cryptsetup mailing list <cryptsetup@lists.linux.dev> or in Issues project section <https://gitlab.com/cryptsetup/cryptsetup/-/issues/new>.

Please attach output of the failed command with --debug option added.

SEE ALSO

Cryptsetup FAQ <https://gitlab.com/cryptsetup/cryptsetup/wikis/FrequentlyAskedQuestions>

cryptsetup(8), integritysetup(8) and veritysetup(8)

CRYPTSETUP

Part of cryptsetup project <https://gitlab.com/cryptsetup/cryptsetup/>.